Exam : **HPE7-A01**

Title : Aruba Certified Campus Access Professional Exam

https://www.passcert.com/HPE7-A01.html

1.Your Aruba CX 6300 VSF stack has OSPF adjacency over SVI 10 with LAG 1 to a neighboring device. The following configuration was created on the switch:

```
vlan 20,30,40
!
interface vlan 20
     ip address 10.10.20.1/24
!
interface vlan 30
     ip address 10.10.30.1/24
!
interface vlan 40
     ip address 10.10.40.1/24
```

A)

```
vlan 20, 30,40
   ospf passive
```

B)

```
interface vlan 20,30,40
   ip ospf passive
```

C)

```
router ospf 1
 area 0
 passive-interface
   vlan 20.30.40
```

D)

```
router ospf 1
   area 0
      redistribute local
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

Explanation:

The correct configuration for OSPF adjacency over SVI 10 with LAG 1 to a neighboring device is shown in Option C.

The configuration includes the following steps:

* Create a VLAN 10 and assign it a name and an IP address.
* Create a LAG 1 and assign it a name and a mode of dynamic or static.
* Add member ports to LAG 1 and enable the LAG interface.
* Assign VLAN 10 as the untagged VLAN for LAG 1.
* Enable OSPF on the switch and assign it a router ID.
* Create an OSPF area 0 and add SVI 10 as an interface in that area.

Option A is incorrect because it does not enable OSPF on the switch or create an OSPF area. Option B is incorrect because it assigns VLAN 10 as the tagged VLAN for LAG 1, which is not compatible with SVI 10.

Option D is incorrect because it does not add member ports to LAG 1 or enable the LAG interface.
References:
https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-BD3E0A5F-FE4C-4B9B-BE1D-FE7D
https://techhub.hpe.com/eginfolib/Aruba/OS-CX_10.04/5200-6692/GUID-BD3E0A5F-FE4C-4B9B-BE1D-FE7D

2.The customer needs a network hardware refresh to replace an aging Aruba 5406R core switch pair using spanning tree configuration with Aruba CX 8360-32YC switches.
What is the benefit of VSX clustering with the new solution?
A. stacked data-plane
B. faster MSTP converge processing
C. dual Aruba AP LAN port connectivity for PoE redundancy
D. dual control plane provides better resiliency
Answer: D
Explanation:
VSX clustering is a feature that allows two Aruba CX switches to operate as a single logical device, providing high availability, scalability, and simplified management.
VSX clustering has several benefits over spanning tree configuration, such as:
* Dual control plane provides better resiliency. Unlike stacking, where switches share a single control plane, VSX switches have independent control planes that synchronize their states over an inter-switch link (ISL). This means that if one switch fails or reboots, the other switch can continue to operate without affecting traffic flows or network services.
* Active-active forwarding provides better performance. Unlike spanning tree, where some links are blocked to prevent loops, VSX switches use all available links for forwarding traffic, providing load balancing and increased bandwidth utilization.
* Multichassis LAG provides better redundancy. Unlike single-chassis LAG, where all member ports belong to one switch, VSX switches can form multichassis LAGs with downstream or upstream devices, where member ports are distributed across both switches. This provides link redundancy and seamless failover in case of switch or port failure.
References: https://www.arubanetworks.com/assets/tg/TG_VSX.pdf

3.What is enabled by LLDP-MED? (Select two.)
A. Voice VLANs can be automatically configured for VoIP phones
B. APs can request power as needed from PoE-enabled switch ports
C. iSCSI client devices can request to have flow control enabled
D. GVRP VLAN information can be used to dynamically add VLANs to a trunk
E. iSCSI client devices can set the required MTU setting for the port.
Answer: A B
Explanation:
These are two benefits enabled by LLDP-MED (Link Layer Discovery Protocol - Media Endpoint Discovery).
LLDP-MED is an extension of LLDP that provides additional capabilities for network devices such as VoIP phones and APs. One of the capabilities is to automatically configure voice VLANs for VoIP

phones, which allows them to be placed in a separate VLAN from data devices and receive QoS and security policies.
Another capability is to request power as needed from PoE-enabled switch ports, which allows APs to adjust their power consumption and performance based on the available power budget. The other options are incorrect because they are either not enabled by LLDP-MED or not related to LLDP-MED.
References:
https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/wlan-qos/lldp-me
https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/wlan-rf/poe.htm

4.A company deployed Dynamic Segmentation with their CX switches and Gateways After performing a security audit on their network, they discovered that the tunnels built between the CX switch and the Aruba Gateway are not encrypted. The company is concerned that bad actors could try to insert spoofed messages on the Gateway to disrupt communications or obtain information about the network.
Which action must the administrator perform to address this situation?
A. Enable Secure Mode Enhanced
B. Enable Enhanced security
C. Enable Enhanced PAPI security
D. Enable GRE security
Answer: B
Explanation:
To address the situation of unencrypted tunnels between the CX switch and the Aruba Gateway, the administrator must enable Enhanced security on both devices. Enhanced security is a feature that provides encryption and authentication for GRE tunnels between CX switches and Aruba Gateways using IPSec.
Enhanced security can be enabled globally or per tunnel on both devices using CLI commands or Web UI options. The other options are incorrect because they either do not provide encryption or authentication for GRE tunnels or do not exist as features.
References:
https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch05.html
https://www.arubanetworks.com/assets/ds/DS_AOS-CX.pdf

5.What is true regarding 802.11k?
A. It extends radio measurements to define mechanisms for wireless network management of stations
B. It reduces roaming delay by pre-authenticating clients with multiple target APs before a client roams to an AP
C. It provides mechanisms for APs and clients to dynamically measure the available radio resources.
D. It considers several metrics before it determines if a client should be steered to the 5GHz band, including client RSSI
Answer: C
Explanation:
802.11k is a standard that provides mechanisms for APs and clients to dynamically measure the available radio resources in a wireless network. 802.11k defines radio resource management (RRM)

functions, such as neighbor reports, link measurement, beacon reports, etc., that allow APs and clients to exchange information about the RF environment and make better roaming decisions. The other options are incorrect because they describe other standards, such as 802.11r, 802.11v, or 802.11ax.
References:
https://www.arubanetworks.com/assets/wp/WP_WiFi6.pdf
https://www.arubanetworks.com/assets/ds/DS_AP510Series.pdf

6.What is an Aruba-recommended best practice for hardening that only applies to Aruba CX 6300 series switches with dedicated management ports?
A. Implement a control plane ACL to limit access to approved IPs and/or subnets
B. Manually enable Enhanced Security Mode from a console session.
C. Disable all management services on the default VRF.
D. Create a dedicated management VRF, and assign the management port to it.
Answer: D
Explanation:
This is an Aruba-recommended best practice for hardening that only applies to Aruba CX 6300 series switches with dedicated management ports. A dedicated management port is a physical port that is used exclusively for out-of-band management access to the switch. A dedicated management VRF is a virtual routing and forwarding instance that isolates the management traffic from other traffic on the switch. By creating a dedicated management VRF and assigning the management port to it, the administrator can enhance the security and performance of the management access to the switch. The other options are incorrect because they either do not apply to switches with dedicated management ports or do not follow Aruba-recommended best practices.
References:
https://www.arubanetworks.com/assets/ds/DS_AOS-CX.pdf
https://www.arubanetworks.com/assets/tg/TB_ArubaCX_Switching.pdf

7.A customer is using stacked Aruba CX 6200 and CX 6300 switches for access and a VSX pair of Aruba CX 8325 as a collapsed core 802 1X is implemented for authentication. Due to the lack of cabling, some unmanaged switches are still in use Sometimes devices behind these switches cause network outages The switch should send a warning to the helpdesk when the problem occurs You have been asked to implement an effective solution to the problem.
What is the solution for this?
A. Configure spanning tree on the Aruba CX 8325 switches Set the trap-option
B. Configure loop protection on all edge ports of the Aruba CX 6200 and CX 6300 switches No trap option is needed
C. Configure loop protection on all edge ports of the Aruba CX 6200 and CX 6300 switches Set up the trap-option
D. Configure spanning tree on the Aruba CX 6200 and CX 6300 switches No trap option is needed
Answer: C
Explanation:
This is the correct solution to the problem of devices behind unmanaged switches causing network outages due to loops. Loop protection is a feature that allows an Aruba CX switch to detect and prevent loops by sending loop protection packets on each port, LAG, or VLAN on which loop protection is enabled.

If a loop protection packet is received by the same switch that sent it, it indicates a loop exists and an action is taken based on the configuration. Loop protection should be configured on all edge ports of the Aruba CX 6200 and CX 6300 switches, which are the ports that connect to end devices or unmanaged switches. The trap-option should be set up to send a warning to the helpdesk when a loop is detected. The other options are incorrect because they either do not configure loop protection or do not set up the trap-option.
References:
https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7540/GUID-99A8B276-0DA3-4458-AF
https://www.arubanetworks.com/techdocs/AOS-CX/10.05/HTML/5200-7540/GUID-D8613BDE-CD21-4B83-85

8.Which feature supported by SNMPv3 provides an advantage over SNMPv2c?
A. Transport mapping
B. Community strings
C. GetBulk
D. Encryption
Answer: D
Explanation:
Encryption is a feature supported by SNMPv3 that provides an advantage over SNMPv2c. Encryption protects the confidentiality and integrity of SNMP messages by encrypting them with a secret key. SNMPv2c does not support encryption and relies on community strings for authentication and authorization, which are transmitted in clear text and can be easily intercepted or spoofed. Transport mapping, community strings, and GetBulk are features that are common to both SNMPv2c and SNMPv3.
References:
https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/snmp/snmp.htm
https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/snmp/snmpv3.htm

9.You are configuring Policy Based Routing (PBR) for a subnet that will be used to test a new default route for your network Traffic originating from 10.2.250.0/24 should use a new default route to 10.1.1.253. Other non-default routes for this subnet should not be affected by this change.
What are two parts of the solution for these requirements? (Select two.)
A)

```
pbr-action-list def_route_test
    default-nexthop 10.1.1.253/24
```

B)

```
class ip test_subnet
    10 match any 10.2.250.0/24 any
policy def_route_test_policy
    10 class ip test_subnet action pbr def_route_test
interface vlan 100
    ip address 10.2.250.0/24
    apply policy pbr_test routed in
```

C)

```
class ip test_subnet
    10 match any 10.2.250.0 255.255.255.0 any
policy def_route_test_policy
    10 class ip ip_test_subnet action pbr def_route_test
interface vlan 100
    ip address 10.2.250.0/24
    apply policy pbr_test routed out
```

D)

```
pbr-action-list def_route_test
    default-nexthop 10.1.1.253
    interface null
```

E)

```
pbr-action-list def_route_test
    nexthop 10.1.1.253
    interface null
```

A. Option A
B. Option B
C. Option C
D. Option D
E. Option E

Answer: A E

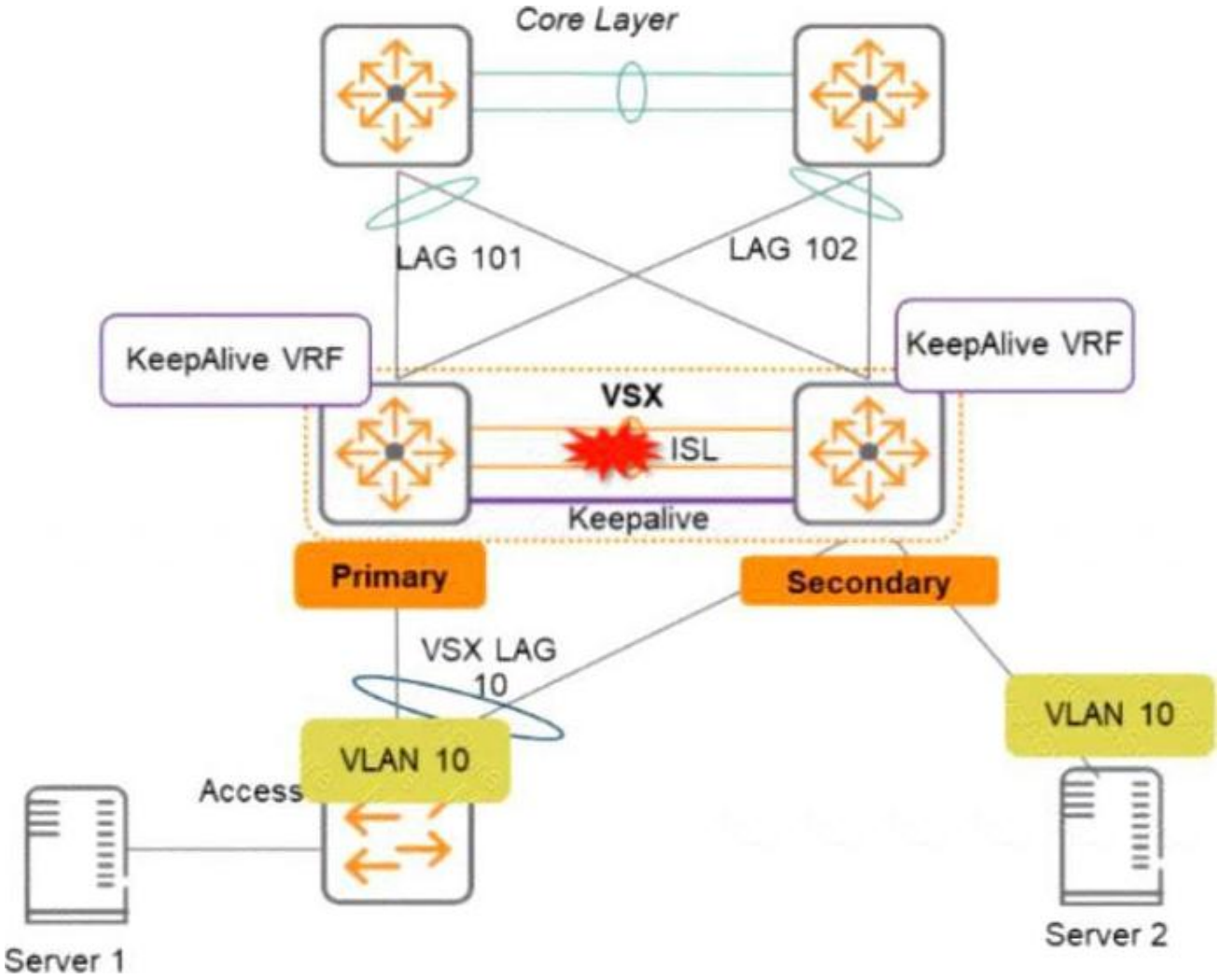
Explanation:

These are the correct parts of the solution for the requirements of configuring Policy Based Routing (PBR) for a subnet that will be used to test a new default route for your network. Option A defines a PBR policy named test-default-route with a rule named new-default-route that matches traffic from source IP address 10.2.250.0/24 and sets the next hop IP address to 10.1.1.253. Option E applies the PBR policy to VLAN 10 interface, which is the subnet that needs to use the new default route. The other options are incorrect because they either do not match the correct traffic or do not set the correct next hop.

References:

https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch02.html
https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-ch03.html

10.Two AOS-CX switches are configured with VSX at the the Access-Aggregation layer where servers attach to them An SVI interface is configured for VLAN 10 and serves as the default gateway for VLAN 10. The ISL link between the switches fails, but the keepalive interface functions. Active gateway has been configured on the VSX switches.



What is correct about access from the servers to the Core? (Select two.)

A. Server 1 can access the core layer via the keepalrve link

B. Server 2 can access the core layer via the keepalive link

C. Server 2 cannot access the core layer.

D. Server 1 can access the core layer via both uplinks

E. Server 1 and Server 2 can communicate with each other via the core layer

F. Server 1 can access the core layer on only one uplink

Answer: D E

Explanation:

These are the correct statements about access from the servers to the Core when the ISL link between the switches fails, but the keepalive interface functions. Server 1 can access the core layer via both uplinks because it is connected to VSX-A, which is still active for VLAN 10. Server 2 can also access the core layer via its uplink to VSX-B, which is still active for VLAN 10 because of Active Gateway feature. Server 1 and Server 2 can communicate with each other via the core layer because they are in the same VLAN and subnet, and their traffic can be routed through the core switches. The other statements are incorrect because they either describe scenarios that are not possible or not relevant to the question. References: https://www.arubanetworks.com/techdocs/AOS-CX/10.04/HTML/5200-6728/bk01-

11.What is an OSPF transit network?

A. a network that uses tunnels to connect two areas
B. a special network that connects two different areas
C. a network on which a router discovers at least one neighbor
D. a network that connects to a different routing protocol
Answer: B
Explanation:
OSPF is a link-state routing protocol that divides a network into areas. An area is a logical grouping of routers that share the same link-state information. Area 0 is the backbone area that connects all other areas. A transit network is a special network that connects two different areas. A transit network must belong to Area 0 and have at least two OSPF routers attached to it. A transit network allows traffic from one area to pass through another area without changing the area ID.
References:
https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html
https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13703-8.html

12.Which Aruba AP mode is sending captured RF data to Aruba Central for waterfall plot?
A. Hybrid Mode
B. Air Monitor
C. Spectrum Monitor
D. Dual Mode
Answer: C
Explanation:
Spectrum Monitor is an Aruba AP mode that is sending captured RF data to Aruba Central for waterfall plot.
Spectrum Monitor is a mode that allows an AP to scan all channels in both 2.4 GHz and 5 GHz bands and collect information about the RF environment, such as interference sources, noise floor, channel utilization, etc. The AP then sends this data to Aruba Central, which is a cloud-based network management platform that can display the data in various formats, including waterfall plot. Waterfall plot is a graphical representation of the RF spectrum over time, showing the frequency, amplitude, and duration of RF signals. The other options are incorrect because they are either not AP modes or not sending RF data to Aruba Central.
References:
https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-overview/spect
https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/1-overview/water
https://www.arubanetworks.com/products/network-management-operations/aruba-central/